IN THE CLAIMS:

1. (Currently amended) A method in a node for managing ~~authorized~~ attempts to access the node, the method comprising:

receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

dropping the packet without a response to the source if the first key does not match the second key;

storing information from the packet; and

sending the information to a selected recipient in response to a selected event.

2. (Original) The method of claim 1, wherein the selected event is a request from the recipient for the information.

3. (Original) The method of claim 1, wherein the selected event is an occurrence of a trap.

4. (Original) The method of claim 1, wherein the selected event is a periodic event.

5. (Original) The method of claim 1 further comprising:

incrementing a counter source if the first key does not match the second key.

6. (Currently amended) The method of claim ~~1~~ 5, wherein the selected event occurs when the counter exceeds a threshold value.

7. (Currently amended) The method of claim 1, wherein the ~~key is a partition key~~ node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

8. (Original) The method of claim 1, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

9. (Currently amended) The method of claim ~~1~~ 7, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet.

10. (Currently amended) A method in a node for reporting access violations, the method comprising:

receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

dropping the packet without a response to the source if the received authentication information is unverified;

storing information from the packet; and

sending the information to a selected recipient in response to a selected event.

11. (Currently amended) The method of claim 10, wherein the ~~information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address~~ node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

12. (Currently amended) A data processing system comprising:

a bus system;

a channel adapter unit connected to a system area network fabric;

a memory connected to the bus system, wherein the memory includes as set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node; determine whether the first key matches a second key for the node; drop the packet without a response to the source if the first key does not match the second key; store information from the packet; and send the information to a selected recipient in response to a selected event.

13. (Currently amended) A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node;

determining means for determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

dropping means for dropping the packet without a response to the source if the first key does not match the second key;

storing means for storing information from the packet; and

sending means for sending the information to a selected recipient in response to a selected event.

14. (Original) The node of claim 13, wherein the selected event is a request from the recipient for the information.

15. (Original) The node of claim 13, wherein the selected event is an occurrence of a trap.

16. (Original) The node of claim 13, wherein the selected event is a periodic event.

17. (Original) The node of claim 13 further comprising:

incrementing means for incrementing a counter source if the first key does not match the second key.

18. (Currently amended) The node of claim ~~13~~ 17, wherein the selected event occurs when the counter source exceeds a threshold value.

19. (Currently amended) The node of claim 13, wherein the ~~key is a partition key~~ node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

20. (Original) The node of claim 13, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

21. (Currently amended) The node of claim ~~13~~ 19, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet.

22. (Currently amended) A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

verifying means for verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

dropping means for dropping the packet without a response to the source if the reccived authcntication information is unverified;

storing means for storing information from the packet; and

sending means for sending thc information to a selected recipient in response to a selected event.

23. (Currently amended) The node of claim 22, wherein the ~~information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address~~ node comprises at least onc device private to the node and at least one device shared with at least one of the partitions of the multi-partition network .

24. (Currently amended) A computer program product in a computer readable medium for use in a node for managing ~~authorized~~ attempts to access the node, thc computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes a first kcy, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that thc node can determine which of the partitions of the multi-partitioned network can access thc nctwork node;

second instructions for determining whether thc packet is from a partition authorizcd to access the node by determining whether the first key matchcs a second key for thc node;

third instructions for dropping the packet without a response to the source if the first kcy does not match the second key;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipicnt in response to a selected event.

25. (Currently amended) A computer program product in a computer readable medium for use in a node for reporting access violations, the computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

second instructions for verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

third instructions for dropping the packet without a response to the source if the received authentication information is unverified;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipient in response to a selected event.